Part I Getting Started

Chapter 1: *Introduction to Strong Authentication at Fermilab*

Many of you are aware that Fermilab is in the process of implementing new methods for users to access the computers at the FNAL site. The purpose of this introduction is to summarize the plan and explain what it means for you as Fermilab computer users, system administrators, and software developers, and what you will need to do to prepare for this change.

Chapter 2: *Fermilab Computing Policy Issues*

The full text of the Fermilab Policy on Computing is maintained at `http://www.fnal.gov/cd/main/cpolicy.html`. Section 4 addresses Strong Authentication. In this chapter we summarize the important points.

Chapter 3: *Kerberos Principals and Passwords*

In this chapter we discuss choosing and obtaining a strengthened realm userid (called a *Kerberos principal*) and a Kerberos password.

Chapter 1: Introduction to Strong Authentication at Fermilab

Many of you are aware that Fermilab is in the process of implementing new methods for users to access the computers at the FNAL site. The purpose of this introduction is to summarize the plan and explain what it means for you as Fermilab computer users, system administrators, and software developers, and what you will need to do to prepare for this change.

1.1 Computing on the World Wide Web

The landscape of the computing environment has changed dramatically from the days when the Internet was primarily the domain of the academic research community. The same explosive growth in computing hardware, network connectivity, and capable software that has enabled HEP to tackle the daunting computing challenges of our field have led to a tremendous increase in the pool of participants on the Internet. There has been increasing "urbanization" of the Internet. This means, among other things, that the previous methods of access control are insufficient for today's needs.

1.2 Strong Authentication

The new access methods involve a concept known as "strong authentication".

> Strong authentication is a system of verifying the identities of networked users, clients and servers without transmitting passwords over the network. It does not require that the network be protected. Both parties in a connection must demonstrate knowledge of some "secret" to establish their identities.

The strong authentication service implemented at Fermilab is the Kerberos Network Authentication Service V5. Kerberos (throughout the manual, "Kerberos" refers to Kerberos V5) is a network authentication protocol designed to serve as a trusted third-party authentication service. It verifies the

identity of a user or a network service (users and services are collectively called *principals*) on an unprotected network using conventional cryptography in the form of a shared secret key. In addition to establishing identity (authentication), it supports encrypted network connections, thereby providing confidentiality.

The "heart" of a Kerberos installation is the Key Distribution Center (KDC). All the computers associated with a KDC make up what's called a *strengthened realm*. At Fermilab, the strengthened realm for UNIX machines is called FNAL.GOV. For Windows 2000, you will use FERMI.WIN.FNAL.GOV. The KDC's main functions include:

- Maintaining a database of users and services within its realm
- Authenticating users by way of exchanging tickets between clients and services in the strengthened realm

A short summary of some key points of Fermilab's implementation of strong authentication is included at the end of this letter. For more information, see Appendix A: *Implementation Details of Strong Authentication at Fermilab* and Appendix B: *About the Kerberos Network Authentication Service V5*.

The current plan requires that the strong authentication be fully deployed at FNAL by the end of calendar 2001.

1.3 Why is Fermilab implementing strong authentication?

There have been several computer security breaches at Fermilab and other DOE facilities. Our funding agencies are requiring Fermilab to demonstrate that it is implementing a computer security system that exercises tight control over who uses the lab's computers and network.

In response, Fermilab has issued revisions to its Computing Policy that detail responsibilities and requirements for accessing computing resources at Fermilab. The Computing Policy is provided online at `http://www.fnal.gov/cd/main/cpolicy.pdf`. We provide the relevant information from the policy in more readable language in Chapter 2: *Fermilab Computing Policy Issues*.

This manual seeks to explain the implementation of Strong Authentication at Fermilab. Where there appear to be conflicts, the Policy prevails.

1.4 What do you need to know and do ?

Virtually all machines at FNAL will require Kerberos authentication for network access. You will need to be able to satisfy that authentication requirement in order to gain access. The work you need to do depends on the role you play in your computing use, e.g., user or administrator, on the OS you use, and on whether you connect from your machine over the network to other machines or not.

If you bring a machine from your university to FNAL, the machine must be Kerberized if you wish to participate in the strengthened realm. We highly recommend that you participate, as it makes your access to other FNAL machines much simpler.

For those of you at a university or other off-site location, you may include your machine in the FNAL Kerberos realm as well. Off-site machines have different requirements for doing so.

1.4.1 General User

As a general UNIX or Windows user, you should expect that the maintainer of your computer has provided the basic tools and installation necessary to configure the machine as a member of Fermilab's strengthened realm.

Your responsibilites are listed below:

General User Responsibilities	Where to find Information
(Recommended) Understand the broad outlines of Fermilab's Strong Authentication policy.	Read the entire Part I: *Getting Started*, especially Chapter 2: *Fermilab Computing Policy Issues*.
Obtain a Kerberos principal (an identifier for the realm, akin to a login name) and a Kerberos password.	See section 3.1.2 *Requesting a Principal*, or go straight to the online form at `http://www.fnal.gov/cd/forms/strongauth.html`.
Obtain a CRYPTOCard if necessary, learn how to use it, and care for it properly.	You can find out what a CRYPTOCard is used for and determine whether you need one by reading section 5.5 *Connecting from a NonKerberized Machine: Portal Mode*. Care and use of CRYPTOCards are described in Appendix : *Using your CRYPTOCard*.

General User Responsibilities	Where to find Information
Change your initial Kerberos password to an acceptable one of your choosing within 30 days of receipt.	If your experiment or group doesn't have a Kerberized machine set up yet, or if you don't have an encrypted connection to a Kerberized machine, log into fnkerb.fnal.gov to change your password and to get acquainted with Kerberos. If you have an account on fnalu, you have an account on fnkerb, and vice-versa. See sections 3.2.2 *Choosing a Kerberos Password*, 3.2.3 *Changing your Kerberos Password* and 5.1 *Trying Out Kerberos on fnkerb.fnal.gov.*
Learn how to obtain your login credentials.	How to do this depends on whether you're logging in to a Kerberized machine at the console or over the network, on what software you're using, and on other factors.)
Learn how to use your login credentials without exposing them to theft.	See section(s) of Chapter 5: *Accessing Kerberized Machines* appropriate to your operating system(s), and Chapter 11: *Encrypted vs. Unencrypted Connections.*
And last but not least: Treat your Kerberos password as a sacred object!! • Do not tell anyone your Kerberos password. • Do not write it down anywhere that someone could find it. • Do not put it in a file (encrypted or not). • As a usual practice, type it only at the console of a system on which you authenticate; do not pass it over the network, even encrypted, on a regular basis. • On the rare occasions when you need to authenticate remotely, verify that all connections in the chain are encrypted. • Do not use the same character string as your Kerberos password for any other password or any other object. (One exception: W2K domain password; see below) • If you mistakenly type it over an unencrypted channel, change it immediately!	

Windows Desktop Users

Labwide migration for Windows desktops from the NT4 domain to the Windows 2000 domain is in early stages of implementation. The W2K domain structure supports Kerberos authentication. For information on this, see *Migration from NT4 Domain to Windows 2000 Domain* from the Windows desktop tutorial at `http://www.fnal.gov/docs/strongauth/presentations/WINdesktop/w2kadmin.html` and see the *Windows 2000 at Fermilab* homepage at `http://www-win2k.fnal.gov/`.

1.4.2 System Administrator

As a system administrator (including those who administer their own machines), you need to do and understand everything the general user does, and in addition, you must understand how to setup the Kerberos tools and how to properly configure the machine for the strengthened realm. For users of the Computing Division's UPS/UPD environment, much of this has been automated. Also a number of system vendors are providing Kerberos as a standard option within their OS installation. You may use whichever tools you prefer as long as the result complies with Fermilab policy. The obligation is on you, the adminstrator, to understand your own configuration well enough to ensure compliance. The chapters in the Administrator part of the manual provide detailed instructions on many common circumstances at the lab.

1.4.3 Developer

You as an application or system developer need to understand the principles of strong authentication, and the Fermilab Computing Policy in detail. It is your responsibility to design systems and software that enhance the security of Fermilab's computing systems and to improve our ability to withstand the onslaught of attackers who would misuse our resources.

1.5 What advantages will you see?

One big advantage is that you will have *one* id, known as your Kerberos principal, and *one* password that can be used anywhere at the lab (eventually two principals: name@FNAL.GOV and name@FERMI.WIN.FNAL.GOV). This simplifies life considerably. You still need authorization to use machines to which you log in (an account or an entry in an access control list), but there are no passwords that need to be locally maintained anymore.

Once you are authenticated on a system, you can move from one strengthened machine to another without having to type your password again.

And, most importantly, the computers *will be more secure* from abuse by outsiders.

1.6 What advantages does Kerberos have over other possible solutions?

In Kerberos V5, the password-checking (authentication) happens in one place, and the end systems need not store any information which can be used to try to guess a password. Further, Kerberos allows a single point of disabling an unauthorized or wayward user on all systems in the strengthened realm. This feature satisfies one of Fermilab's obligations to the DOE.

In ssh, as in standard UNIX, each end system has to store information sufficient to check the password, which is therefore also sufficient to try to guess the password. If the RSA authentication method is used, the RSA keys can give access to various accounts, and there's no way to know with certainty who possesses which keys. In the event of a compromise of a private key, there's no mechanism for locating every host on which the corresponding public key appears.

1.7 How does Kerberos work?

Kerberos authentication operates by the exchange of tickets that allow access to all services by the user in the strengthened realm:

1) Password-derived information is stored in the central Key Distribution Server (KDC).

2) User logs into Kerberized desktop computer, not over the network. User requests authentication either automatically at login or via **`kinit`** command after login. Entry of Kerberos password is required. Or, user logs into nonKerberized machine, and proceeds to connect to a Kerberized machine over the network using a CRYPTOCard-generated password to authenticate.

3) Password is used to derive a key to encrypt the exchanges between local host and KDC, but is not transmitted between them.

4) Upon authentication, user gets "ticket" from KDC.

5) User can now log in to other strengthened hosts without typing a password again. By *forwarding* tickets at login, the user can do all of the following without typing a password:

   · connect from one strengthened host to another

   · obtain AFS tokens

   · **`ksu`** to other accounts as permitted

1.8 How do you obtain a Kerberos Principal?

There's a form online at `http://www.fnal.gov/cd/forms/strongauth.html`. But first, read more about principals in Chapter 3: *Kerberos Principals and Passwords*.

After you get a principal, you'll need to change your Kerberos password. If your experiment or group doesn't have a Kerberized machine set up yet, or if you don't have an encrypted connection to a Kerberized machine, log into fnkerb.fnal.gov or any of the FNALU machines to change your password and to get acquainted with Kerberos. Fnkerb is described in section 5.1 *Trying Out Kerberos on fnkerb.fnal.gov*. If you have an account on FNALU, you have an account on fnkerb, and vice-versa.

Chapter 2: Fermilab Computing Policy Issues

The full text of the Fermilab Policy on Computing is maintained at `http://www.fnal.gov/cd/main/cpolicy.html`. Section 4 addresses Strong Authentication. In this chapter we summarize the important points.

2.1 The Strong Authentication Policy in a Nutshell

By the end of 2001, we expect to complete the implementation of Kerberos V5 on the UNIX computers at Fermilab. Migration of the Windows NT domain to the Kerberized Windows 2000 domain may stretch into 2002. Our working definition of *computer*, as regards strong authentication, is: "any machine to which you can log in, and on which you can run arbitrary code".

Kerberos authentication is currently **not** required for:

- uses which involve only reading public information (e.g., via the web)
- anonymous FTP
- email
- entering information into a web or database form, in most cases

All other network accesses to computers on the Fermilab site must be preceded by Kerberos V5 authentication if the access is comparable to shell or FTP service.

Compliance can be achieved in different ways:

- Run Kerberos authentication
- Remain unKerberized, but remove incoming network services
- (not for desktops) Remain unKerberized, but require users to gain access through a computer that either:
  - requires Kerberos authentication, or
  - is isolated from the general network and physically accessible only to individuals carrying a valid Fermilab ID card.

Furthermore, an on-site system may not be configured to accept a reusable login password over the network.

Telnet, ssh, and other connection program daemons must not prompt for or accept a Kerberos password. To log in over the network:

- Authenticate on local desktop machine prior to remote login (and forward tickets if possible, or on rare occasions run `kinit` after **encrypted** remote login)
- From nonKerberized node, authenticate using your CRYPTOCard

Off-site computers participating in Fermilab's strengthened realm must enforce secure access mechanisms, but they are not required to use Kerberos V5.

2.2 Authentication Guidelines for On-site vs. Off-site Machines

First let us distinguish between an authentication method and a transport mechanism as it pertains to on-site versus off-site machines:

- *Authentication methods* serve to identify the user; examples include: Kerberos credentials, CRYPTOCards, passwords, RSA keys, and IP addresses + "privileged ports". For on-site machines, only Kerberos credentials and CRYPTOCards are allowed as authentication methods. For off-site machines, any secure method is acceptable.
- Ssh, telnet, FTP, and so on are the network connection programs, or the *transports*, and none is forbidden per se. The restriction is imposed on the authentication methods, and the transport is restricted only in that it must support an acceptable authentication method.

The following table summarizes Fermilab's policy regarding how strong authentication may be achieved on UNIX machines in the Fermilab strengthened realm depending on whether the machine is on- or off-site:

Authentication Method	Allowed for ON-site System?	Allowed for OFF-site System?
Kerberos V5 strong authentication via kerberos product (Fermi kerberos or from other source)	yes	yes
Kerberos-based authentication via software other than Kerberos (e.g., Kerberos-based ssh)	yes	yes
CRYPTOCard challenge/response authentication	yes	yes
Clear-text reusable passwords entered at system console	yes	yes

Authentication Method	Allowed for ON-site System?	Allowed for OFF-site System?
Other non-reusable and/or non-clear-text password authentication over the network	no	yes
Non-Kerberos strong authentication (e.g., RSA or equivalent authentication) followed by obtaining Kerberos credentials via kinit over encrypted connection	no	no
Standard UNIX security (e.g., rhosts-based authentication)	no	no
Cleartext passwords (Kerberos or otherwise) transmitted over network	no	no

2.3 Transient Machines

Laptop machines brought in by visitors for short periods of time (e.g., one week) do not need to be registered or Kerberized. Visitors may use their host's accounts (with host's permission) at the host's responsibility, although sharing Kerberos passwords is not allowed. Local accounts that allow access only at the console will be permitted for visitors (no NIS accounts). Facilities created primarily for visitors may be granted exemptions from the requirement for Kerberos-validated users.

2.4 Obtaining an Exemption from the Policy

Exemptions from the strong authentication policy are granted on a case-by-case basis. Exemptions will be considered only for cases which involve a large effort for compliance *and* a small risk for noncompliance. If this applies to your situation, see your experiment's or your division's computer security representative to request an exemption; he or she will forward your request to the Fermilab Computer Security Coordinator (FCSC). The duration of any exemption granted is determined on a case-by-case basis.

2.5 Compliance with Policy

First, a few notes regarding good user practices:

- Fermilab's policy seeks to limit the transmission of users' Kerberos passwords over the network, even over encrypted connections. We therefore urge you to install software on your machine that allows you to authenticate to Kerberos locally, and to forward tickets automatically to remote hosts. You are allowed to type your Kerberos password over an encrypted link on an occasional basis with the **`kinit`** or **`kpasswd`** commands (e.g., when initially changing your password), however as a regular practice, please authenticate locally and forward your credentials.
- Do not disclose your Kerberos password to anybody, and do not ever type it over an unencrypted connection. Try to minimize the number of times per day or per week that you need to type it for any reason.
- In short, following the usage recommendations and installation instructions provided throughout this manual will keep you in compliance with Fermilab's Computing Policy as regards Strong Authentication.

Regarding penalties for noncompliance, we quote from section 4 of the Fermilab Policy on Computing (at `http://www.fnal.gov/cd/main/cpolicy.html`):

"Hosts found to be noncompliant may be barred from obtaining Kerberos tickets from our realm. If the noncompliance is deliberate or extremely careless it may be deemed to constitute blatant disregard for computer security."

Chapter 3: Kerberos Principals and Passwords

In this chapter we discuss choosing and obtaining a strengthened realm userid (called a *Kerberos principal*) and a Kerberos password.

3.1 Your Kerberos Principal

In order to access a machine in the FNAL.GOV realm, you need to have a special identifier for the realm, called a *Kerberos principal*[1], and an associated Kerberos password. A principal is essentially a realm userid, used for authentication to the realm. You must have a valid Fermilab ID in order to get one. In addition to a principal, you must have an account on each machine that you plan to use in the realm. There are significant conveniences if your principal and your account name are the same, as we discuss in section 3.1.1 *Choosing a Principal Name*.

The system administrator of a strengthened machine may require that authorized users obtain a *<username>/root* instance of their Kerberos principal in order to access sensitive accounts on the system. The root instance has tighter restrictions placed on it (see section 9.2 *Ticket Management*). If your sytem administrator tells you it's required, use the same form as indicated in section 3.1.2 *Requesting a Principal* to request one.

3.1.1 Choosing a Principal Name

The Kerberos Strong Authentication system is expanding to include all computer systems across the site. Your Kerberos principal will be used for authentication sitewide. It is to your benefit to have one login id (account name) common to all systems that you use, and for that login id to match your Kerberos principal. The Computing Division is strongly encouraging this

1. Note for sysadmins: if you have an account and a standard UNIX password (in the `passwd` file or NIS map) on a Kerberized machine, but no principal or Kerberos password, you can still log in and use non-Kerberized services. You can do this only at the console. (From any other terminal, the Kerberized system responds in portal mode, described in section 5.5 *Connecting from a NonKerberized Machine: Portal Mode*, and you have no option to enter your UNIX password.)

practice for ease of use. (For users new to Fermilab, your FNAL email address and your login name for all machines will be created to match your principal, by default.) With this in mind, we provide the following guidelines for choosing a Kerberos principal:

> New principals should be chosen to be eight or fewer characters, and may include a variety of characters. Please use only lowercase letters (and optionally any numbers 0 through 9). **Do not use the characters "at" (@), forward slash (/), or period (.) in principal names**.

In Appendix C: *More about Choosing a Principal Name*, we present information for users who have pre-existing account names and/or an email address at Fermilab, and for whom the above guidelines are not straightforward to follow.

3.1.2 Requesting a Principal

Use the online *Form to Request Kerberos Principal and/or Related Items* at `http://www.fnal.gov/cd/forms/strongauth.html`. Guidance is provided on the form as to which items you may need in addition to a principal.[1]

3.2 Your Kerberos Password

Once your request for a principal on the FNAL.GOV realm has been approved, you must stop by WH8NE (Yolanda Valadez' office) to receive your initial Kerberos password. An exception is granted for off-site visitors (whose Fermilab ID is a VID): you can get it over the telephone (630-840-8118); you will be asked a question to verify your identity.[2]

You are required to change the initial password within 30 days of receipt, and once a year (actually every 400 days) thereafter.

---

1. Note that if you obtained a principal for the PILOT.FNAL.GOV realm, you do **not** need to get a new principal (or password) for the transition from the PILOT.FNAL.GOV realm to FNAL.GOV.

2. For principals that were migrated from the PILOT.FNAL.GOV realm to the production realm on May 10, 2001, the existing pilot realm password and expiration date were replicated in the production realm. A password *change* in one realm after that date will not be reflected in the other realm.

Even if you use a CRYPTOCard exclusively, you need to change your Kerberos password as stated above in order to continue accessing machines in the FNAL.GOV realm!

3.2.1 Important! Please Read!

Please treat your Kerberos password as an inviolable object. Never give your password to anybody for any reason. Doing so constitues a policy violation. If you really need to give someone access to your account (this practice is discouraged, by the way), add the person's principal to your `.k5login` or `.k5users` file as described in section 9.3 *Account Access by Multiple Users*.

Typing in your Kerberos password should ideally be done infrequently (i.e., no more than once each day). Do not type it in carelessly. You are allowed to type your Kerberos password over an **encrypted** link on an occasional basis (e.g., when initially changing your password), however as a regular practice, please authenticate locally and forward your credentials to remote systems.

Windows 2000 domain-only users: type your password **only** at the Windows login prompt.

3.2.2 Choosing a Kerberos Password

In contrast to the principal (which ideally should match your login name on each machine and your email address), your Kerberos password must be unique. That is, in order to avoid exposing your Kerberos password, it must be different from the passwords you use for any other purpose (with the single exception of your Fermilab Windows 2000 domain Kerberos password).

The Fermilab Computer Security Team has imposed some restrictions on passwords in accordance with DOE guidelines. Currently, a password for the FNAL.GOV strengthened realm is required to contain a minimum of ten characters from at least two of the following five classes: lowercase letters, uppercase letters, numbers, punctuation, and all other characters. Passwords for /root principals must contain a minimum of 11 characters including at least three of the five classes. Passwords the system considers "bad" will be rejected. (Passwords are checked against the "cracklib" dictionary, which will often surprise you by its thoroughness!)

Need some ideas for thinking up a good password?[1] Remember, a good password is one you can remember, but that no one else can easily guess. Examples of passwords that would be good *if they weren't listed in this manual* include:

---

1. These ideas were lifted from MIT's Kerberos V5 User's Guide (C) 1996, local copy stored at `http://www-dcd.fnal.gov/computersecurity/StrongAuth/UserDocs/user-guide.html`.

- some initials, like “GykoR-66.” for “Get your kicks on Route 66.”
- an easy-to-pronounce nonsense word, like “slaRooBey” or “krang-its”
- a misspelled phrase, like “2HotPeetzas!” or “ItzAGurl!!!”

Note: Don’t actually use any of the above passwords. They’re only meant to show you how to make up a good password. Passwords that appear in a manual are the first ones intruders will try.

3.2.3 Changing your Kerberos Password

If possible, change your password at the console of a machine, not over a network connection. If this is not possible, then before changing your password, **verify that you are using an encrypted connection!** How do you know if your connection is encrypted? See Chapter 11: *Encrypted vs. Unencrypted Connections* for some help.

We repeat: You are required to change your initial password within 30 days of its creation and roughly once a year thereafter in order to continue having access to machines in the strengthened realm, no matter what access method you use. The **kinit** program warns you if your password is within 30 days of its expiration date, and as of **kerberos** v1_2, the **kerberos** login program includes this warning as well.

The Computing Division has set up terminals in two locations for people to change their Kerberos passwords. There is one terminal outside of WH8NE, another is in the email center in Wilson Hall, ground floor, north end.

If you don’t have a secure connection over which to change your password, find someone who does, and borrow his or her command prompt (yes, you can change it from someone else’s account; just give your principal name as an argument).

If your initial password expires, you can still change it as long as you remember what it was, but you cannot use CRYPTOCard access while it remains expired. If you forget your initial password before you get around to changing it, stop by WH8NE (or off-site call 630-840-8118) and ask Yolanda Valadez to reset it (but please try to change it right away!).

UNIX/Linux/Cygwin

To change your password, run the **`kpasswd`** command.

On strengthened UNIX systems running AFS, there are two **`kpasswd`** commands, one for AFS (`/usr/afsws/bin/kpasswd`) and one for Kerberos (`/usr/krb5/bin/kpasswd`). Your $PATH should be set such that the Kerberos **`kpasswd`** comes first. Kerberos is implemented at Fermilab such that your AFS tokens will be obtained automatically. If you are unsure which **`kpasswd`** is being invoked, force the system to use the Kerberos version by running **`setup kerberos`** first.

```
% setup kerberos
```

Then run **kpasswd**. If borrowing someone else's account or if your principal does not match your login id, include your principal name as an argument.

```
% kpasswd [<principal_name>]
```

```
kpasswd: Changing password for aheavey@FNAL.GOV.
Old password:                 <--- type your initial password here.
kpasswd: aheavey@FNAL.GOV's password is controlled by the policy default,
which
requires a minimum of 10 characters from at least 2 classes (the five classes
are lowercase, uppercase, numbers, punctuation, and all other characters).
New password:                 <--- type your new password here.
New password (again):         <--- type your new password here for confirmation.
Kerberos password changed.
```

If you choose a password that is too short, you will see this error message:

```
kpasswd: New password is too short.
Please choose a password which is at least 10 characters long.
```

If it's long enough but you haven't met the multiple-class requirement, you'll see:

```
kpasswd: New password does not have enough character classes.
The character classes are:
        - lower-case letters,
        - upper-case letters,
        - digits,
        - punctuation, and
        - all other characters (e.g., control characters).
Please choose a password with at least 2 character classes.
```

If the password has expired, you'll need to get access to a machine running **kpasswd** some other way (e.g., find a friend or use a local account) to change it.

Windows (with WRQ® Reflection software installed)

Here we assume you are running the **WRQ® Reflection** software for **Windows** as described in Chapter 19: *Installing and Configuring WRQ® Reflection on a Windows System*. To change your Kerberos password via the **Reflection** application:

- (If you run W2K or NT4, and installed WRQ® using the automated script, skip this first step.) First update the Windows services file by executing `\\Pckits\WRQ\services.bat`. For Win95 or 98, you must copy it manually from `\\Pckits\WRQ\` (target directory may vary).
- Next, navigate to **START > PROGRAMS > REFLECTION > UTILITIES > KERBEROS MANAGER** to open the **Reflection Kerberos Manager** application. From the **TOOLS** menu select **CHANGE PASSWORD...** and change it.

Windows (with Exceed 7.0 and MIT Kerberos)

Here we assume you are running **Exceed 7** with the **MIT Kerberos** software for Windows as described in Chapter 22: *Installing MIT Kerberos on Windows, for use with Exceed 7 and FileZilla*.

Note: The **CHANGE PASSWORD** utility in **Leash32** does not work, and **`kpasswd`** in the Command Prompt works for the AFS password. Consequently, changing your password under this configuration requires typing your password over a network connection. Try to find a machine on which you can do it locally, instead. Only use this as a last resort.

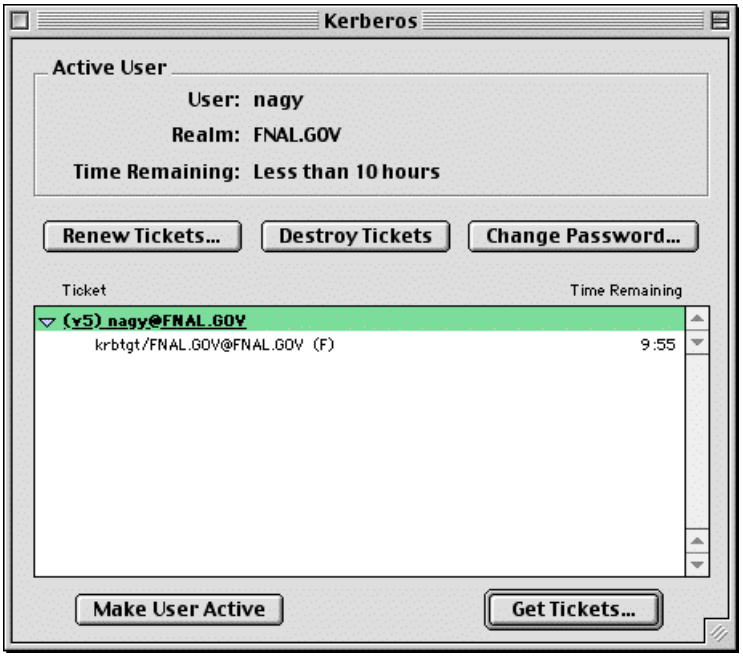
To change your Kerberos password:

Make your connection to your UNIX host using a telnet profile with Kerberos enabled as outlined in section 22.5 *Configuring the Exceed 7 Telnet Application*. Verify that encryption is set. Use the **`kpasswd`** command to change your Kerberos password, as described for UNIX, earlier in this section.

Macintosh

Here we assume you are running the **MIT Kerberos** software for Macintosh as described in Chapter 24: *Installing and Configuring MIT Kerberos on a Macintosh System*. To change your Kerberos password:

1) Invoke the **Kerberos Control Panel** (from **CONTROL PANELS** under the Apple menu, from the **KERBEROS MENU** in the menu bar, or from the **KERBEROS CONTROL STRIP** module).



2) Select a username and realm and click **GET TICKETS** for which you will have to provide your current (or initial) Kerberos password.

3) Click on the ticket to highlight it, then click **CHANGE PASSWORD** and enter the old and new passwords on the pop-up screen which appears.